Procédé de chiffrement/déchiffrement d'un message et dispositif associé.

La présente invention concerne un procédé de sécurisation et d'identification de messages sur un réseau, ainsi qu'un dispositif sécurisé correspondant.

Un réseau est constitué d'un ensemble de dispositifs émetteur/ récepteur adaptés à échanger des messages par exemple par un bus numérique, par radiodiffusion ou par l'intermédiaire du réseau Internet.

Pour sécuriser la circulation de messages transmis sur le réseau entre un dispositif émetteur/récepteur sécurisé, couramment appelé autorité de certification, et un dispositif émetteur/récepteur client, il est connu de chiffrer les messages à l'aide de clés de chiffrement.

En général, le dispositif émetteur des messages dispose d'une clé de chiffrement et le dispositif récepteur d'une clé de déchiffrement correspondante.

Le chiffrement des messages a deux types principaux d'applications :

- la sécurisation d'un message qui consiste en une substitution à un texte clair, d'un texte inintelligible et inexploitable,

- l'identification d'un message qui consiste à garantir l'origine et l'intégrité d'un message transitant sur le réseau par utilisation d'une signature numérique.

Dans ces deux types d'applications, il convient de minimiser les risques d'interception et de déchiffrement frauduleux des messages par un tiers, ou de falsification par l'apposition frauduleuse d'une signature.

Différents procédés de cryptographie ont donc été proposés pour éviter les chiffrements ou déchiffrements non autorisés.

Par exemple, des procédés de cryptographie dits symétriques ont été proposés. Dans ces procédés, la même clé, appelée clé secrète est utilisée pour le chiffrement et le déchiffrement d'un message. Cependant, ces procédés sont faiblement sécurisés car lorsque la clé secrète est découverte, l'ensemble des dispositifs émetteur/récepteur du réseau est corrompu.

Une amélioration à de tels procédés consiste à utiliser des techniques dites de dérivation de clés symétriques. La figure 1 illustre un exemple d'utilisation de cette technique. Elle représente schématiquement l'architecture d'une autorité de certification 100 et d'un appareil client 102 donné d'un réseau d'appareils aptes à communiquer avec cette autorité de certification.

Selon la technique de dérivation de clés symétriques, chaque appareil client 102 possède sa propre clé de chiffrement/déchiffrement KD_i, différente des clés des autres appareils du réseau. Cette clé est calculée ou dérivée à partir d'un identifiant CID_i stocké dans chaque appareil client 102 et d'une clé dite maîtresse MK connue de l'autorité de certification 100 uniquement. Cette clé dérivée est utilisée à la fois pour chiffrer et déchiffrer un message.

La clé dérivée KD_i est générée au départ par l'autorité de certification puis mémorisée dans chaque appareil client de manière sécurisée. Ensuite, avant chaque échange de message m avec un appareil client donnée, l'autorité de certification 100 demande à l'appareil client 102 son identifiant CID_i puis recalcule la clé dérivée KD_i du dispositif client concerné par application d'une fonction de dérivation à l'identifiant CID_i et à la clé maîtresse MK. Puis, l'autorité de certification chiffre (notation « E ») ou déchiffre (notation « D ») le message à l'aide de la clé dérivée calculée. La notation $E\{KD_i\}(m)$ correspond au chiffrement du message m à l'aide de la clé KD_i.

Un exemple de techniques dites de dérivation de clés symétriques utilisées pour l'identification d'un message est décrit dans le document WO 02/19613.

Cette technique est plus sécurisée qu'un procédé symétrique classique car lorsqu'une clé dérivée d'un appareil client donné est piratée, l'ensemble des appareils clients du réseau n'est pas corrompu car le pirate ne peut pas calculer les clés dérivés des autres appareils. Toutefois, cette technique est coûteuse car elle nécessite la sécurisation de l'ensemble des appareils clients.

Par ailleurs, des procédés de cryptographie asymétrique ont été proposés. Ces procédés se caractérisent par l'emploi d'un couple de clés de chiffrement et de déchiffrement non identiques appelées clé publique/clé privée.

La figure 2 illustre un exemple d'utilisation d'un procédé asymétrique dans lequel un appareil client 202, 203 est apte à transmettre un message chiffré à une autorité de certification 200.

Selon ce procédé asymétrique, chaque appareil client 202, 203 du réseau d'appareils clients comporte une clé publique $PubC_i$, $PubC_j$ qui lui est propre et qu'il utilise pour chiffrer un message m à transmettre. L'autorité de certification 200 stocke dans une base de données toutes les clés privées

correspondant aux clés publiques des appareils clients. Les clés privées sont dans l'exemple de la figure 2 mémorisées par l'autorité de certification 200 avec les identifiants de chaque appareil client. Lorsqu'un appareil client 203 veut transmettre un message m chiffré à l'autorité de certification 200, il transmet, en plus du message m chiffré avec sa clé publique E $\{PubC_i\}$ (m), son identifiant CID_i de sorte que l'autorité de certification puisse retrouver la clé privée correspondante $PrivC_i$. Le message m est alors déchiffré à l'aide de la clé privée $PrivC_i$.

Avantageusement, de tels procédés asymétriques ne nécessitent pas la sécurisation des appareils clients. En effet, le piratage d'un appareil client et donc la découverte de sa clé publique de chiffrement n'autorise pas le déchiffrement du message envoyé. Seule la clé privée correspondant spécifiquement à cette clé publique de chiffrement permet le déchiffrement du message.

Cependant, le principal inconvénient de ce type de procédé asymétrique réside dans la nécessité pour l'autorité de certification de gérer une base de données dans laquelle sont stockées l'ensemble des clés privées de tous les appareils clients du réseau. Cette base de données nécessite une mémoire de stockage importante. De plus, la recherche d'une clé privée dans cette base de données implique des temps de transfert de message assez long qui handicapent les échanges.

En variante, des procédés asymétriques ont été proposés, dans lesquels, un unique couple de clés privée/publique chiffre l'ensemble des messages. Les appareils clients du réseau contiennent donc tous la même clé publique et l'autorité de certification stocke une unique clé privée. Toutefois, ces procédés ne sont pas suffisamment sécuritaires car le piratage de la clé privée corrompt l'ensemble du réseau des appareils clients.

Le but de la présente invention est de fournir un procédé de chiffrement/déchiffrement alternatif qui présente un niveau de sécurité élevé sans nécessiter le stockage et la gestion d'une base de données de clés asymétriques.

A cet effet, la présente invention a pour objet un procédé de chiffrement/déchiffrement d'un message à échanger entre un émetteur et un récepteur par l'intermédiaire d'un réseau de communication, l'émetteur et le

récepteur étant l'un et l'autre d'un dispositif sécurisé et d'un dispositif client défini dans un réseau de dispositifs clients, le procédé comprenant les étapes de :

- réalisation d'opérations de cryptographie asymétrique par le dispositif sécurisé et par le dispositif client défini respectivement à l'aide d'une clé privée et d'une clé publique, la clé privée étant différente de la clé publique, et

- envoi d'au moins une donnée publique du dispositif client défini vers le dispositif sécurisé,

caractérisé en ce que le procédé comporte en outre, lors de chaque émission/réception d'un message chiffré par le dispositif sécurisé, une étape de détermination de la clé privée correspondant à la clé publique du dispositif client défini, à partir d'une clé maîtresse secrète stockée dans le dispositif sécurisé, et de la ou de chaque donnée publique envoyée par le dispositif client défini.

Avantageusement, ce procédé utilise les techniques de dérivation de clés symétriques associées au procédé de cryptographie asymétrique. Ainsi, les techniques de dérivation ne seront pas utilisées pour générer une clé dérivée secrète mais pour générer une clé privée d'un couple de clés privée/publique.

Un autre objet de l'invention consiste en un dispositif sécurisé apte à échanger des messages avec un dispositif client défini d'un réseau de dispositifs clients, sur un réseau de communication, le dispositif sécurisé étant apte à recevoir au moins une donnée publique propre audit dispositif client défini et envoyée par celui-ci préalablement à tout échange de messages, le dispositif sécurisé comprenant des moyens de réalisation d'opérations de cryptographie asymétrique à l'aide d'une clé privée correspondant à une clé publique stockée dans le dispositif client défini caractérisé en ce qu'il comprend, en outre des moyens de stockage sécurisés d'une clé maîtresse, et des moyens de détermination de ladite clé privée à partir de la clé maîtresse et de la ou de chaque donnée publique envoyée.

L'invention sera mieux comprise et illustrée au moyen d'un exemple de réalisation et de mise en œuvre, nullement limitatif, en référence aux figures annexées sur lesquelles :

- la figure 1 est une vue schématique de l'architecture d'une autorité de certification et d'un appareil récepteur aptes à échanger des messages chiffrés selon un procédé de dérivation de clés symétriques connu,

- la figure 2 est une vue schématique de l'architecture d'une autorité de certification et d'un appareil émetteur aptes à échanger des messages chiffrés selon un procédé de chiffrement asymétrique connu,

- la figure 3 est une vue schématique de l'architecture d'un dispositif sécurisé selon un exemple de réalisation de l'invention pour la génération d'un couple de clés privée/publique lors d'une phase d'initialisation des appareils du réseau,

- la figure 4 est un diagramme récapitulatif des différentes étapes du procédé de chiffrement/déchiffrement lors de la phase d'initialisation, selon l'exemple de réalisation de l'invention,

- la figure 5 est une vue schématique de l'architecture d'un dispositif sécurisé et d'un dispositif client pour la sécurisation d'un message selon l'exemple de réalisation de l'invention, et

- la figure 6 est un diagramme récapitulatif des différentes étapes du procédé de chiffrement/déchiffrement pour la sécurisation d'un message selon l'exemple de réalisation de l'invention,

- la figure 7 est une vue schématique de l'architecture d'un dispositif sécurisé et d'un dispositif client pour l'identification d'un message, selon un exemple de réalisation de l'invention, et

- la figure 8 est un diagramme récapitulatif des étapes du procédé de chiffrement/déchiffrement pour l'identification d'un message selon l'exemple de réalisation de l'invention.

La figure 3 représente schématiquement l'architecture d'un dispositif sécurisé 1 et d'un dispositif client C_l.

Le dispositif sécurisé 1 comprend un générateur de nombres aléatoires 2, une mémoire 3 de stockage d'une clé maîtresse, un module de calcul 4 d'une partie d_l de la clé privée et un module de calcul 5 d'une clé publique $PubC_l$.

Le générateur 2 de nombres aléatoires est apte à générer d'une part un nombre susceptible de constituer la clé dite maîtresse MK et d'autre part, une pluralité de nombres CID_l aptes à identifier les dispositifs clients du réseau.

Préférentiellement, la clé dite maîtresse MK a une longueur de 128 bits et les identifiants CID_i, CID_j des dispositifs clients C_i, C_j ont une longueur de 64 bits.

Par ailleurs, le générateur 2 est également apte à générer au hasard deux grands nombres premiers impairs, distincts p et q de 512 bits utilisés pour le calcul de la clé publique par le module de calcul 5.

La mémoire 3 du dispositif sécurisé est non volatile de type « ROM » ou « EEPROM » ou équivalent. Elle est apte à stocker la clé maîtresse MK générée par le générateur 2. Comme la clé maîtresse est une clé secrète connue uniquement par le dispositif sécurisé, la mémoire 3 de stockage de cette clé est avantageusement hautement sécurisée afin de garantir la sécurité des messages échangés.

Le module de calcul 4 est apte à déterminer une partie d'une clé privée d'un couple de clés privée/publique. Généralement, une clé privée $PrivC_i$ est une clé mixte constituée de deux parties. La première partie est formée par une partie de la clé publique appelée modulus n_i dans tout algorithme asymétrique. La deuxième partie est couramment appelée exposant secret d_i dans les algorithmes asymétriques de type RSA : $PrivC_i = (n_i, d_i)$. Le module de calcul 4 est apte à calculer la deuxième partie d_i de la clé privée $PrivC_i$ à partir de l'identifiant CID_i du dispositif client C_i et de la clé maîtresse MK.

Le module de calcul 4 comporte préférentiellement une unité de calcul 6 apte à effectuer une fonction de modification de la longueur d'un identifiant CID_i en une extension de l'identifiant notée $ECID_i$. Une fonction d'extension connue appelée MGF peut par exemple être utilisée. Cette fonction permet d'étendre un nombre de 64 bits en un nombre de 1024 bits. Cette fonction est notamment décrite dans le document de RSA Laboratories « PKCS #1v2.1 : RSA Cryptography Standard – June 14, 2002 » disponible à l'adresse Internet suivante : ftp://ftp.rsasecurity.com/pub/pkcs/pkcs-1/pkcs-1v2-1.pdf

Le module de calcul 4 comprend une unité de chiffrement 7 de l'extension de l'identifiant $ECID_i$ à partir de la clé maîtresse MK. Cette unité met en œuvre un algorithme de dérivation symétrique. De façon préférentielle, il s'agit de l'algorithme couramment appelé AES « Advanced Encryption Standard » utilisé en mode CBC. Cet algorithme est décrit dans le document FIPS 197, 26 Novembre, 2001 disponible sur Internet à l'adresse : http : //csrc.nist.gov/publications/fips/fips197/fips-197.pdf.

Avantageusement, le module de calcul 4 comprend également une unité de sélection 8 de l'exposant secret d_i en fonction du résultat ou chiffré $ECID_i$

de l'extension de l'identifiant. Pour sélectionner cet exposant secret d_i, l'unité de sélection 8 utilise une fonction déterministe. Par exemple, cette unité est propre à sélectionner une donnée telle que cette donnée remplisse les critères ci-dessous :

- cette donnée d_i doit être inférieure au résultat $ECID_i$ du chiffrement de l'extension de l'identifiant,

- cette donnée d_i doit être un nombre le plus proche du résultat $ECID_i$ du chiffrement de l'extension de l'identifiant, premier avec une liste de nombres premiers : 2, 3, 5, 7, 11, 13. Eventuellement, cette dernière condition peut être étendue à une liste de nombres premiers plus longue.

Schématiquement, le module de détermination 5 peut être décomposé en deux unités de calculs. Chaque unité étant apte à calculer un élément de la clé publique : $PubC_i = (n_i, e_i)$.

La première unité de calcul 9 est apte à sélectionner deux grands nombres premiers p_i et q_i générés par le générateur de nombres aléatoires 2 de telle manière que $(p_i - 1) \times (q_i - 1)$ est premier avec l'exposant secret d_i. En pratique, on génère d'abord un nombre p_i tel que (p_i-1) soit premier avec d_i puis un nombre q_i tel que (q_i-1) soit premier avec d_i.

Par ailleurs, cette unité de calcul 9 est apte à calculer la première partie de la clé privée appelée modulus n_i tel que $n_i = p_i \times q_i$. Le modulus n_i constitue également un élément de la clé privée $PrivC_i = (n_i, d_i)$.

La seconde unité de calcul 10 utilise un algorithme d'Euclide étendu pour calculer l'autre élément de la clé publique e_i à partir des données secrètes p_i, q_i et d_i. Cet algorithme d'Euclide étendu est notamment décrit dans l'ouvrage « Handbook of Applied Cryptography » de A. Menezes, P. van Oorschot et S. Vanstone, CRC Press, 1996, à la page 67. Cet ouvrage peut être consulté à l'adresse Internet suivante : http://www.cacr.math.uwaterloo.ca/hac/

Plus précisément, on calcule la donnée e_i telle que :

$e_i \times d_i = 1 \bmod (p_i-1) \times (q_i-1)$.

Les dispositifs clients C_i du réseau comportent une mémoire 11 de stockage d'un identifiant CID_i et d'une clé publique $PubC_i = (n_i, e_i)$ ainsi qu'un module de chiffrement asymétrique ou de vérification de signature.

Classiquement, le dispositif sécurisé 1 et les dispositifs clients C_i, C_j de son réseau de communication sont personnalisés ou initialisés pour pouvoir échanger des messages chiffrés.

Les étapes de principe d'un procédé de personnalisation d'un dispositif sécurisé et des dispositifs clients selon l'invention vont maintenant être décrites.

Le procédé de personnalisation selon l'invention, comprend une première étape de génération d'une clé maîtresse unique MK destinée au dispositif sécurisé 1 et d'une pluralité d'identifiants CID_i, CID_j destinés à caractériser ou personnaliser les dispositifs clients C_i, C_j du réseau.

Ce procédé comprend une deuxième étape de calcul d'un couple de clés privée/publique associé à chaque dispositif client. Spécifiquement, la clé privée est obtenue par chiffrement de l'identifiant CID_i de chaque dispositif client C_i à l'aide de la clé maîtresse MK du dispositif sécurisé : $PrivC_i = f\{MK\}(CID_i)$. La clé publique $PubC_i$ correspondante est calculée à partir de la clé privée notamment par application d'une fonction mathématique utilisant par exemple, un algorithme d'Euclide étendu : $PubC_i = F(PrivC_i)$.

Selon une troisième étape du procédé de personnalisation du dispositif sécurisé et des dispositifs clients du réseau, les identifiants CID_i, CID_j générés et les clés publiques $PubC_i$, $PubC_j$ calculées à partir de ceux-ci sont envoyés à chaque dispositif client C_i, C_j du réseau ou sont insérés dans les dispositifs clients lors de leur fabrication.

Enfin, les clés privées correspondantes $PrivC_i$, $PrivC_j$, ainsi que l'ensemble des données intermédiaires ayant permis de calculer les couples de clés privée/publique sont détruites. Ainsi, le dispositif sécurisé ne stocke aucune donnée associée à l'un quelconque de ces dispositifs clients.

Les étapes d'un exemple de réalisation du procédé de personnalisation vont à présent être décrites en liaison avec la figure 4.

Pendant une étape 41 de la phase de personnalisation des dispositifs du réseau, le générateur 2 génère un nombre aléatoire de 128 bits qui constitue la clé maîtresse MK et un nombre de 64 bits apte à devenir l'identifiant CID_i d'un dispositif client C_i à personnaliser.

Lors d'une étape 42, la clé maîtresse MK ainsi générée est stockée dans la mémoire 3 du dispositif sécurisé 1. Cette clé maîtresse MK servira de

base pour le calcul de l'ensemble des couples de clés privée/publique associés à tous les dispositifs clients du réseau.

Lors d'une étape 43, l'unité de calcul 6 étend l'identifiant CID_i d'un dispositif client C_i par un algorithme d'extension pour générer un nombre de 128 bits formant l'extension de l'identifiant $ECID_i$.

L'extension de l'identifiant $ECID_i$ est ensuite chiffrée à l'étape 44 à l'aide de la clé maîtresse MK. Ce chiffrement est réalisé par l'unité de calcul 7 par application d'un algorithme symétrique de type AES.

Puis, lors d'une étape 45, l'unité de sélection 8 sélectionne un nombre formant l'exposant secret d_i.

Au cours des étapes 46 et 47, le module de calcul 5 sélectionne deux grands nombres premiers p_i et q_i et calcule la clé publique $PubC_i = (n_i, e_i)$ à partir de ces nombres et de l'exposant secret d_i.

Une fois la clé publique $PubC_i = (n_i, e_i)$ d'un dispositif client donnée C_i calculée, le dispositif sécurisé 1 la lui envoie de façon sûre et non détaillée ici accompagné de l'identifiant CID_i à l'origine du calcul de cette clé publique à l'étape 48.

L'identifiant CID_i et la clé publique $PubC_i$ sont enregistrés dans la mémoire 11 du dispositif client C_i.

Avantageusement, selon l'invention, la mémoire 11 des dispositifs clients n'a pas besoin d'être sécurisée contre la lecture car la découverte de la clé publique $PubC_i$ et de l'identifiant CID_i ne permet en aucune façon le calcul de la clé privée correspondante $PrivC_i$ ou le calcul d'une autre clé privée ou publique du réseau, de sorte que la sécurité du message chiffré transmis et du réseau de dispositifs récepteur /émetteur est préservée.

En outre, l'identifiant CID_i ainsi que l'ensemble des données calculées à partir de celui-ci et notamment les données secrètes p_i et q_i, l'exposant secret d_i, l'exposant public e_i, le modulus n_i, et l'extension de l'identifiant $ECID_i$ ne sont pas conservés dans la mémoire 3 du dispositif sécurisé 1 et sont détruits à l'étape 49.

En conséquence, le piratage de la clé maîtresse MK ne permet pas le calcul des clés privée/publique associées à un dispositif client donné sans la connaissance de son identifiant.

Le procédé de personnalisation a pour finalité de configurer le dispositif sécurisé et les dispositifs clients de manière à permettre l'échange des messages chiffrés en vue de leur sécurisation ou de leur identification.

Un exemple d'utilisation des dispositifs émetteur/récepteur selon l'invention en référence aux figures 5 et 6 va être décrit à présent.

En particulier, la figure 5 représente l'architecture d'un dispositif client donné C_j apte à envoyer un message chiffré E {Pub C_j} (m) ainsi que l'architecture d'un dispositif sécurisé 1 apte à déchiffrer ce message.

Classiquement, le dispositif client C_j comporte une mémoire 11 non volatile et un module de chiffrement 12.

La mémoire 11 du dispositif client C_j comporte un identifiant CID_j et une clé publique $PubC_j$ composée d'un modulus n_j, et d'une donnée publique e_j.

Le dispositif sécurisé 1 comprend une mémoire 3 dans laquelle la clé maîtresse MK est stockée, un module de calcul 4 de l'exposant secret d_j et un module de déchiffrement 13.

Selon l'invention, le module de chiffrement 12 et le module de déchiffrement 13 utilisent des procédés de cryptographie asymétrique mettant en œuvre des algorithmes tels que par exemple l'algorithme intitulé RSAES-OAEP. Une description de cet algorithme peut être trouvée dans le document « PKCS #1v2.1 : #RSA Crytography Standard » qui a déjà été mentionné précédemment.

Le module de calcul 4 de l'exposant secret d_j comprend les mêmes unités de calcul que le module de calcul 4 utilisé lors de la phase de personnalisation des dispositifs clients. En conséquence, il calcule l'exposant secret d_i à partir de l'identifiant CID_i du dispositif client C_i et de la clé maîtresse MK de la même manière que lors de la phase de personnalisation de sorte que cet exposant secret d_i corresponde toujours à la clé publique $PubC_i$ de chiffrement stockée dans la mémoire 11 du dispositif client C_i.

Le procédé de chiffrement/déchiffrement pour sécuriser un message va être décrit de manière détaillée en liaison avec la figure 6.

Ce procédé comprend une étape 61 de chiffrement du message à transmettre. Ce chiffrement est réalisé par le module de chiffrement 12 du dispositif client C_j à l'aide de la clé publique $PubC_j = (n_j, e_j)$.

E {Pub C_j} (m) = RSAES-OAEP Encrypt {(n_j, e_j)} (m)

Puis, lors d'une étape 62, l'identifiant CID_j et le modulus n_j du dispositif client C_j ainsi que le message chiffré E {Pub C_j } (m) sont envoyés au dispositif sécurisé 1.

Enfin, les unités de calcul 6, 7 et de sélection 8 du module de calcul 4 de l'exposant secret d_j du dispositif sécurisé 1 réalisent une étape de calcul 63 de l'extension de l'identifiant $ECID_j$ à partir de l'identifiant CID_j envoyé par le dispositif client C_j, une étape de chiffrement 64 de l'extension de l'identifiant $ECID_j$ à l'aide de la clé maîtresse MK et une étape de sélection 65 de l'exposant secret d_j à partir du résultat $ECID_i$ du chiffrement de l'extension de l'identifiant. Il est nécessaire que l'unité de sélection 8 utilise les mêmes règles de sélection que celles appliquées lors de la phase de personnalisation des dispositifs clients.

Finalement, le module de déchiffrement asymétrique 13 du dispositif sécurisé 1 réalise une étape 66 de déchiffrement du message à l'aide de la clé privée mixte composée de l'exposant secret calculé d_j et du modulus n_j envoyé par le dispositif client C_j :

m = RSAES - OAEP – Decrypt {(d_j, n_j)} (E {Pub C_j} (m))

Avantageusement le dispositif sécurisé 1 ne conserve aucune donnée liée au dispositif client C_j émetteur d'un message. Spécifiquement, son identifiant CID_j, l'extension $ECID_j$ de son identifiant, son exposant secret d_j et son modulus n_j sont détruits lors de l'étape 67.

Le procédé de chiffrement/déchiffrement de l'invention permet également d'identifier un message par apposition d'une signature par le dispositif sécurisé 1 et vérification de cette signature par un dispositif client C_j à qui est destiné le message signé.

Le procédé de chiffrement/déchiffrement de l'invention utilisé pour identifier l'origine d'un message va être décrit en liaison avec les figures 7 et 8.

La figure 7 représente schématiquement l'architecture d'un dispositif sécurisé 1 et d'un dispositif client C_j .

Le système composé d'un dispositif sécurisé et d'un dispositif client est similaire au système décrit en liaison avec la figure 5. En conséquence, les éléments communs aux figures 5 et 7 reprennent les mêmes références et ne seront pas à nouveau décrits.

En fait, le système dispositif sécurisé/dispositif client comporte les mêmes modules 4 et mémoires 3, 11 hormis le module de déchiffrement 13 du

dispositif sécurisé et le module de chiffrement 12 du dispositif client qui sont remplacés respectivement par un module de génération de signature 14 et par un module de vérification 15 de signature.

Le procédé de chiffrement/déchiffrement utilisé pour la signature d'un message comprend une étape 81 au cours de laquelle le dispositif sécurisé 1 demande l'identifiant CID_j et le modulus n_j au dispositif client C_j à qui il souhaite envoyer un message m signé.

Au cours des étapes 82, 83, et 84, le module de calcul 4 du dispositif sécurisé 1 recalcule l'exposant secret d_j du dispositif client C_j à partir de l'identifiant envoyé CID_j et de la clé maîtresse MK de la même manière que dans le procédé de chiffrement/déchiffrement utilisé pour la sécurisation ou la personnalisation d'un message et décrit précédemment.

Puis, lors d'une étape 85, le module de signature 14 du dispositif sécurisé 1 signe son message à l'aide de l'exposant secret d_j calculé et du modulus n_j envoyé par le dispositif client C_j : $S\{PrivC_j\}(m)$ avec $PrivC_j = (d_j, n_j)$.

Enfin, le dispositif de sécurisation 1 envoie au cours d'une étape 86, un message m ainsi que sa signature $S\{(d_j, n_j)\}(m)$ au dispositif client défini C_j.

Lors d'une étape 87, le module de vérification 15 du dispositif client C_j vérifie la signature du message à l'aide de la clé publique $PubC_j = (n_j, e_j)$ stockée dans sa mémoire 11 et correspondant à la clé privée $PrivC_j = (d_j, n_j)$ en effectuant l'opération :

$V\{PubC_j\}(S\{PrivC_j\}(m)) = 0$ ou 1

Lors d'une étape 88, l'identifiant CID_j du dispositif client défini C_j et les données intermédiaires CID_j, $ECID_j$, d_j et n_j ayant permis de déterminer la clé privée sont détruits par le dispositif sécurisé.

Pour les opérations de signature S et de vérification de signature V, on pourra notamment utiliser l'algorithme RSASSA-PSS qui est décrit dans le document « PKCS#1v2.1 :RSA Cryptography Standard » mentionné plus haut.

REVENDICATIONS

1. Procédé de chiffrement/déchiffrement d'un message à échanger entre un émetteur et un récepteur par l'intermédiaire d'un réseau de communication, l'émetteur et le récepteur étant l'un et l'autre d'un dispositif sécurisé (1) et d'un dispositif client défini (C_i) dans un réseau de dispositifs clients (C_i, C_j), le procédé comprenant les étapes de :

- réalisation d'opérations de cryptographie asymétrique par le dispositif sécurisé (1) et par le dispositif client défini (C_i) respectivement à l'aide d'une clé privée (n_i, d_i) et d'une clé publique (n_i, e_i), la clé privée étant différente de la clé publique, et

- envoi (62, 81) d'au moins une donnée publique (n_i, CID_i) du dispositif client défini (C_i) vers le dispositif sécurisé (1),

caractérisé en ce qu'il comporte en outre, lors de chaque émission/réception d'un message chiffré par le dispositif sécurisé, une étape de détermination de la clé privée (n_i, d_i) correspondant à la clé publique (n_i, e_i) du dispositif client défini (C_i), à partir d'une clé maîtresse secrète (MK) stockée dans le dispositif sécurisé, et de la ou de chaque donnée publique (n_i, CID_i) envoyée par le dispositif client défini (C_i).

2. Procédé de chiffrement/déchiffrement d'un message selon la revendication 1, caractérisé en ce que l'étape d'envoi (62, 81) de la ou de chaque donnée publique comprend une étape d'envoi d'une partie (n_i) de la clé publique, cette partie de la clé publique formant une première partie de la clé privée.

3. Procédé de chiffrement/déchiffrement d'un message selon l'une quelconque des revendications 1 et 2, caractérisé en ce que l'étape d'envoi (62, 81) de la ou de chaque donnée publique comprend une étape d'envoi d'un identifiant (CID_i) du dispositif client (C_i), et l'étape de détermination de la clé privée comprend une étape de calcul d'une seconde partie (d_i) de la clé privée à partir dudit identifiant envoyé.

4. Procédé de chiffrement/déchiffrement d'un message selon la revendication 3, caractérisé en ce que l'étape de détermination de la clé privée (n_i, d_i) correspondant à la clé publique (n_i, e_i) du dispositif client, comprend une étape de chiffrement (44, 64, 83) du résultat ($ECID_i$) d'une fonction appliquée à

l'identifiant (CID_i) du dispositif client défini (C_i), par un algorithme symétrique, à l'aide de la clé maîtresse secrète (MK).

5. Procédé de chiffrement/déchiffrement d'un message selon la revendication 4, caractérisé en ce que l'étape de détermination de la clé privée (n_i, d_i) correspondant à la clé publique (n_i, e_i) du dispositif client, comporte une étape de sélection (45, 65, 84) de la seconde partie (d_i) de la clé privée, par une unité de calcul déterministe (8), à partir du résultat dudit chiffrement du résultat ($ECID_i$) d'une fonction appliquée à l'identifiant (CID_i) du dispositif client défini (C_i).

6. Procédé de chiffrement/déchiffrement d'un message selon la revendication 5, caractérisé en ce que l'étape de sélection de la seconde partie (d_i) de la clé privée, par l'algorithme déterministe, est réalisée par une sélection d'un nombre tel que :

- ce nombre soit inférieur au résultat dudit chiffrement du résultat ($ECID_i$) d'une fonction appliquée à l'identifiant (CID_i) du dispositif client défini (C_i),
- ce nombre soit le plus proche du résultat dudit chiffrement du résultat ($ECID_i$) d'une fonction appliquée à l'identifiant (CID_i) du dispositif client défini (C_i), et soit premier avec une liste de nombres premiers.

7. Procédé de chiffrement/déchiffrement d'un message selon l'une quelconque des revendications 3 à 6, caractérisé en ce qu'il comprend une étape de destruction (49, 67, 87) de l'identifiant (CID_i) du dispositif client défini (C_i) et de toutes les données (p_i, q_i, d_i, $ECID_i$, e_i, n_i) calculées à partir de l'identifiant pour déterminer la clé privée.

8. Procédé de chiffrement/déchiffrement d'un message selon l'une quelconque des revendications précédentes, caractérisé en ce que les opérations de cryptographie comprennent une opération d'identification d'un message comprenant les étapes suivantes :

- signature du message (85), par le dispositif sécurisé (1), à l'aide de la clé privée (n_i, d_i) déterminée pendant l'étape de détermination de la clé privée,
- transmission de la signature du message et du message (86) au dispositif client pour vérification de cette signature, et
- vérification de la signature (87) du message, par le dispositif client, à l'aide de ladite clé publique (n_i, e_i).

9. Procédé de chiffrement/déchiffrement d'un message selon l'une quelconque des revendications précédentes, caractérisé en ce que les

opérations de cryptographie comprennent une opération de sécurisation d'un message comprenant les étapes suivantes :

- chiffrement (61) d'un message (m), par le dispositif client (C_i), à l'aide de la clé publique (n_i, e_i) ,

- transmission (62) du message chiffré au dispositif sécurisé (1), et

- déchiffrement (66) du message chiffré par le dispositif sécurisé (1), à l'aide de la clé privée (n_i, d_i) déterminée pendant l'étape de détermination d'une clé privée.

10. Procédé de chiffrement/déchiffrement d'un message selon l'une quelconque des revendications 3 à 9, caractérisé en ce qu'il comporte une phase préalable de personnalisation dudit dispositif client défini (C_i), qui comprend les étapes suivantes :

- génération, par le dispositif sécurisé (1), d'une clé maîtresse secrète (MK) unique et d'un identifiant (CID_i) propre audit dispositif client défini (C_i) et apte à l'identifier,

- calcul de ladite clé publique (n_i, e_i) du dispositif client défini (C_i) par un module de calcul (5) à partir de la seconde partie (d_i) de la clé privée.

11. Procédé de chiffrement/déchiffrement d'un message selon la revendication 10, dans lequel la phase de personnalisation comporte en outre les étapes suivantes :

- sélection (46) de deux données secrètes constituées de deux grands nombres premiers p_i, q_i, tels que $(p_i-1) \times (q_i-1)$ soit premier avec la seconde partie (d_i) de la clé privée du dispositif client défini (C_i), et

- calcul (48) d'un modulus n_i du dispositif client défini (C_i) tel que :

$n_i = p_i \times q_i$, et

- calcul (48) d'une partie (e_i) de la clé publique par un algorithme d'Euclide étendu à partir de la ou de chaque donnée secrète p_i, q_i et du modulus n_i du dispositif client défini (C_i).

12. Dispositif sécurisé (1) apte à échanger un message avec un dispositif client défini (C_i) d'un réseau de dispositifs clients (C_i, C_j), sur un réseau de communication, le dispositif sécurisé étant apte à recevoir au moins une donnée publique (CID_i, n_i) propre audit dispositif client défini (C_i) et envoyée par celui-ci préalablement à tout échange de messages, le dispositif sécurisé (1) comprenant :

- des moyens de réalisation d'opérations de cryptographie asymétrique à l'aide d'une clé privée (n_i, d_i) correspondant à une clé publique (n_i, e_i) stockée dans le dispositif client défini (C_i)

caractérisé en ce qu'il comprend, en outre :

- des moyens de stockage (3) sécurisés d'une clé maîtresse (MK),

- des moyens (4) de détermination de ladite clé privée (d_i, n_i) à partir de la clé maîtresse (MK) et de la ou de chaque donnée publique (CID_i, n_i) envoyée.

13. Dispositif sécurisé selon la revendication 12, caractérisé en ce que la donnée publique (CID_i, n_i) comprend une partie (n_i) de la clé publique dudit dispositif client défini (C_i) et/ou un identifiant (CID_i) du dispositif client défini.

14. Dispositif sécurisé selon la revendication 13, caractérisé en ce que la clé privée est une clé mixte comprenant une première partie (n_i) correspondant à une partie de la clé publique (n_i, e_i) dudit dispositif client (C_i) défini et une deuxième partie secrète (d_i) calculée à partir de la clé maîtresse (MK) et de l'identifiant (CID_i) du dispositif client défini.

15. Dispositif sécurisé selon l'une quelconque des revendications 12 à 14, caractérisé en ce que les moyens de réalisation d'opérations de cryptographie asymétrique à l'aide de la clé privée (d_i, n_i) déterminée comprennent :

- des moyens de signature (S) d'un message (m), et

- des moyens de chiffrement (E) d'un message (m).

16. Dispositif sécurisé selon l'une quelconque des revendications 14 à 15, dans lequel les moyens de détermination (4) de la clé privée comprennent en outre :

- une unité de chiffrement (7) symétrique, à l'aide de la clé maîtresse (MK), apte à chiffrer le résultat ($ECID_i$) d'une fonction appliquée à l'identifiant (CID_i) du dispositif client défini (C_i), et/ou

- une unité de calcul (8) d'un algorithme déterministe de sélection de la deuxième partie secrète (d_i) de la clé privée à partir du résultat du chiffrement réalisé par l'unité (7) de chiffrement symétrique.

17. Dispositif sécurisé selon l'une quelconque des revendications 14 à 16, caractérisé en ce qu'il comprend outre un moyen d'initialisation des dispositifs clients du réseau, ledit moyen d'initialisation comprenant :

- un moyen de génération (2) aléatoire d'une clé maîtresse unique (MK) et d'une pluralité d'identifiants (CID_j, CID_i) distincts les uns des autres, chaque identifiant étant propre à caractériser un unique dispositif client (C_i) du réseau de dispositif client,

- une unité de calcul (9) apte à sélectionner deux données secrètes (p_i, q_i) en fonction de la valeur de la deuxième partie secrète (d_i) de la clé privée et à calculer une première partie (n_i) de la clé publique, et

- une unité de calcul (10) de la seconde partie (e_i) de la clé publique, par un algorithme d'Euclide Etendue, à partir des données secrètes (p_i, q_i), de la deuxième partie (d_i) de la clé privée et de la première partie (n_i) de la clé publique.

18. Programme d'ordinateur comportant des instructions pour l'exécution des étapes de procédé de chiffrement/déchiffrement d'un message selon l'une quelconque des revendications 1 à 11, lorsque le programme est exécuté sur un dispositif sécurisé réalisé à partir d'un calculateur programmable.

19. Support d'enregistrement utilisable sur un dispositif sécurisé réalisé à partir d'un calculateur programmable sur lequel est enregistré le programme selon la revendication 18.

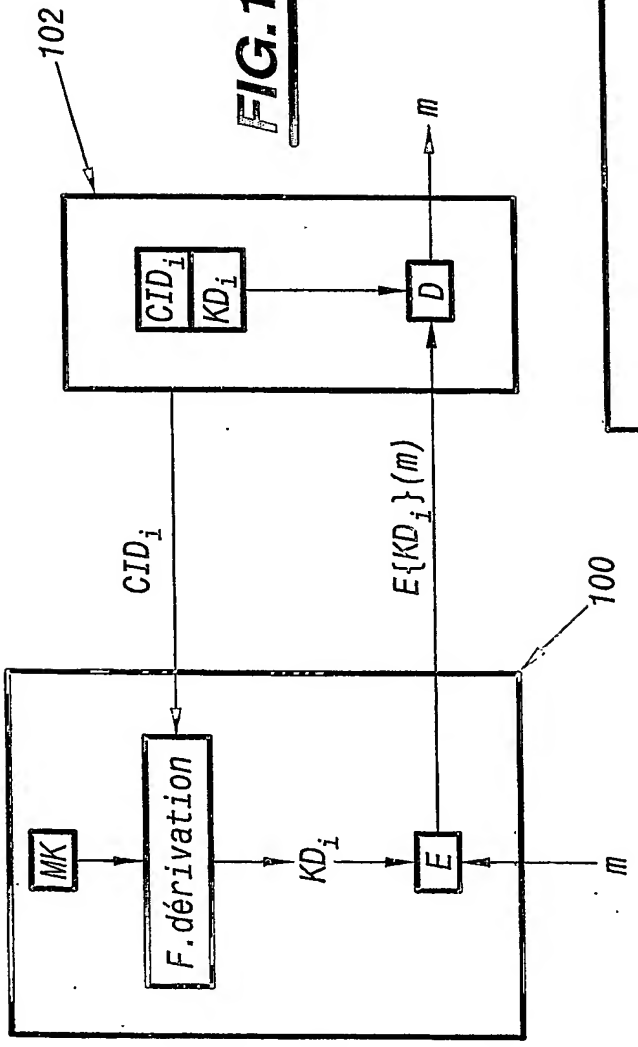
MK
F.dérivation
KD_i
E
m
100
CID_i
$E\{KD_i\}(m)$
102
CID_i
KD_i
D
m

FIG.1

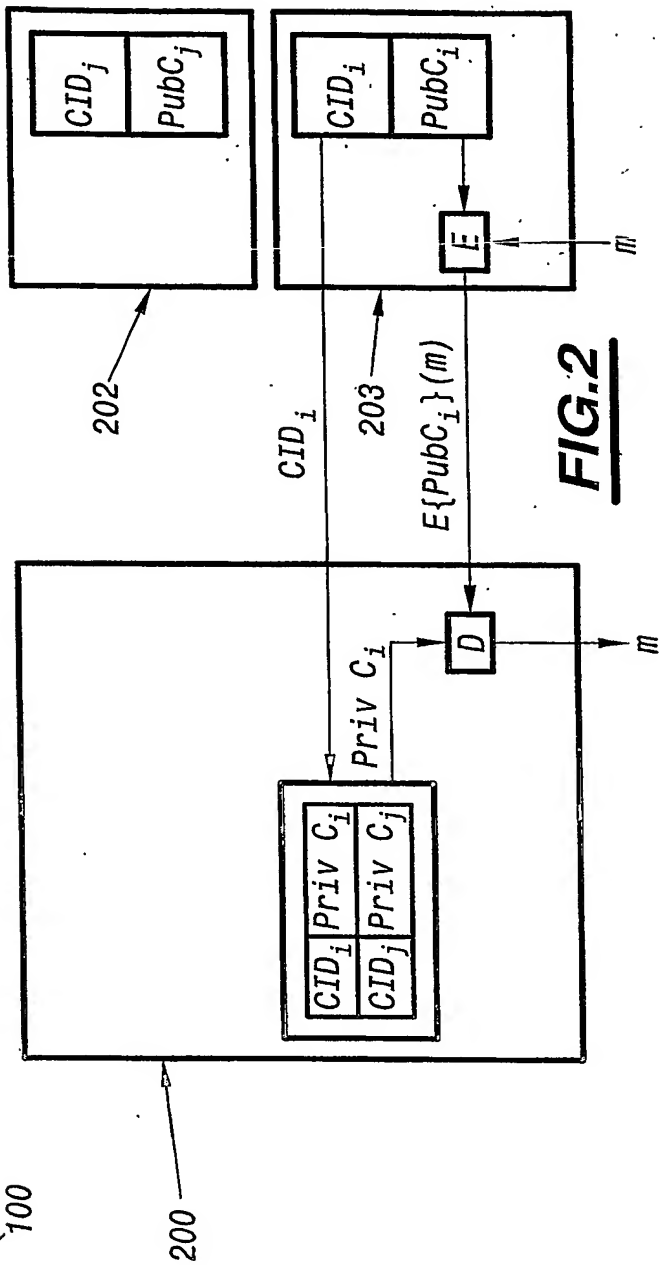
CID_j
$PubC_j$
202
CID_i
$PubC_i$
E
m
CID_i
203
$E\{PubC_i\}(m)$
200
CID_i
$Priv\ C_i$
CID_j
$Priv\ C_j$
D
m

FIG.2

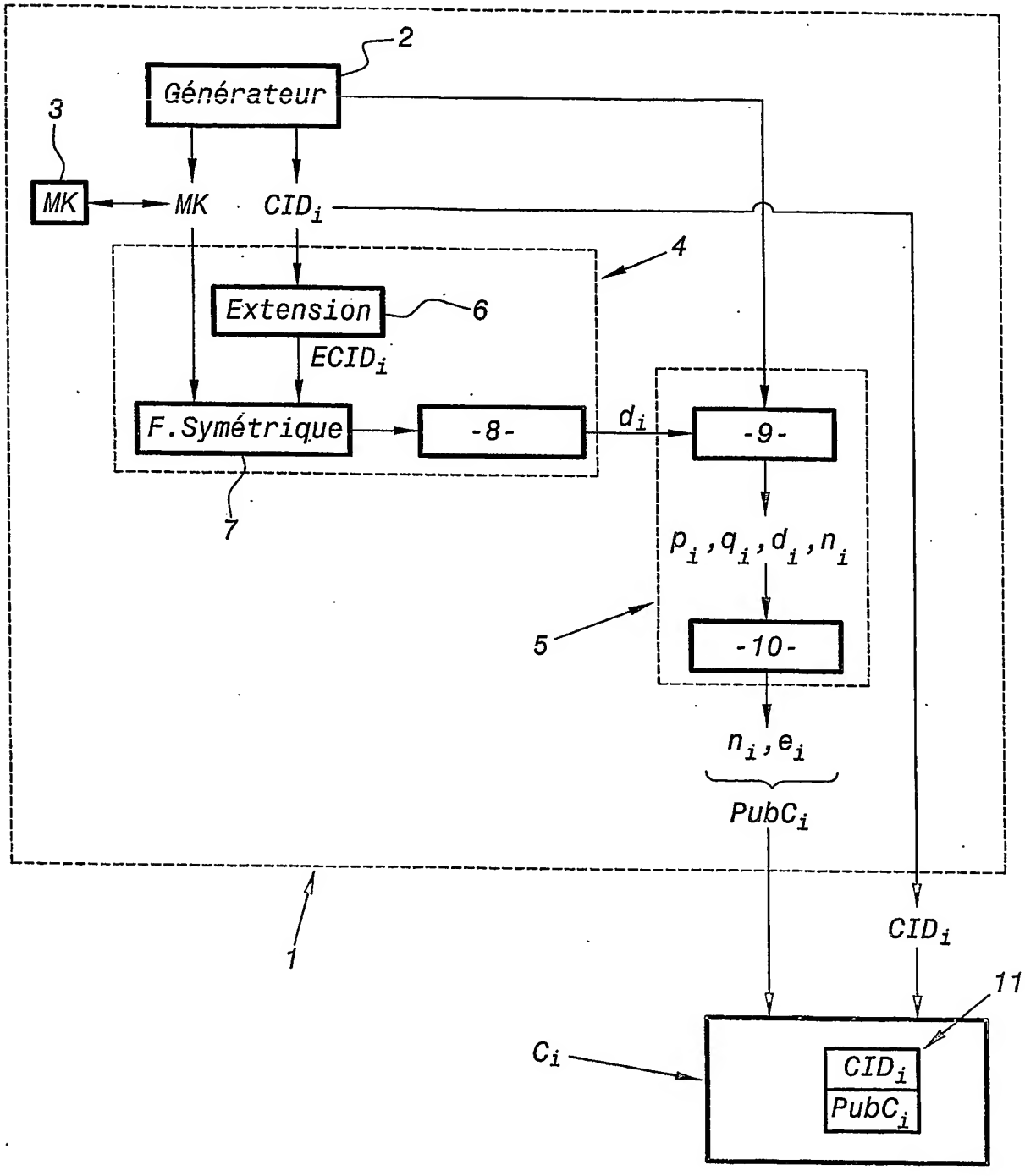
2
Générateur
3
MK
MK
CID_i
4
Extension
6
$ECID_i$
F.Symétrique
-8-
d_i
-9-
p_i, q_i, d_i, n_i
5
-10-
n_i, e_i
$PubC_i$
7
1
CID_i
11
C_i
CID_i
$PubC_i$

FIG.3

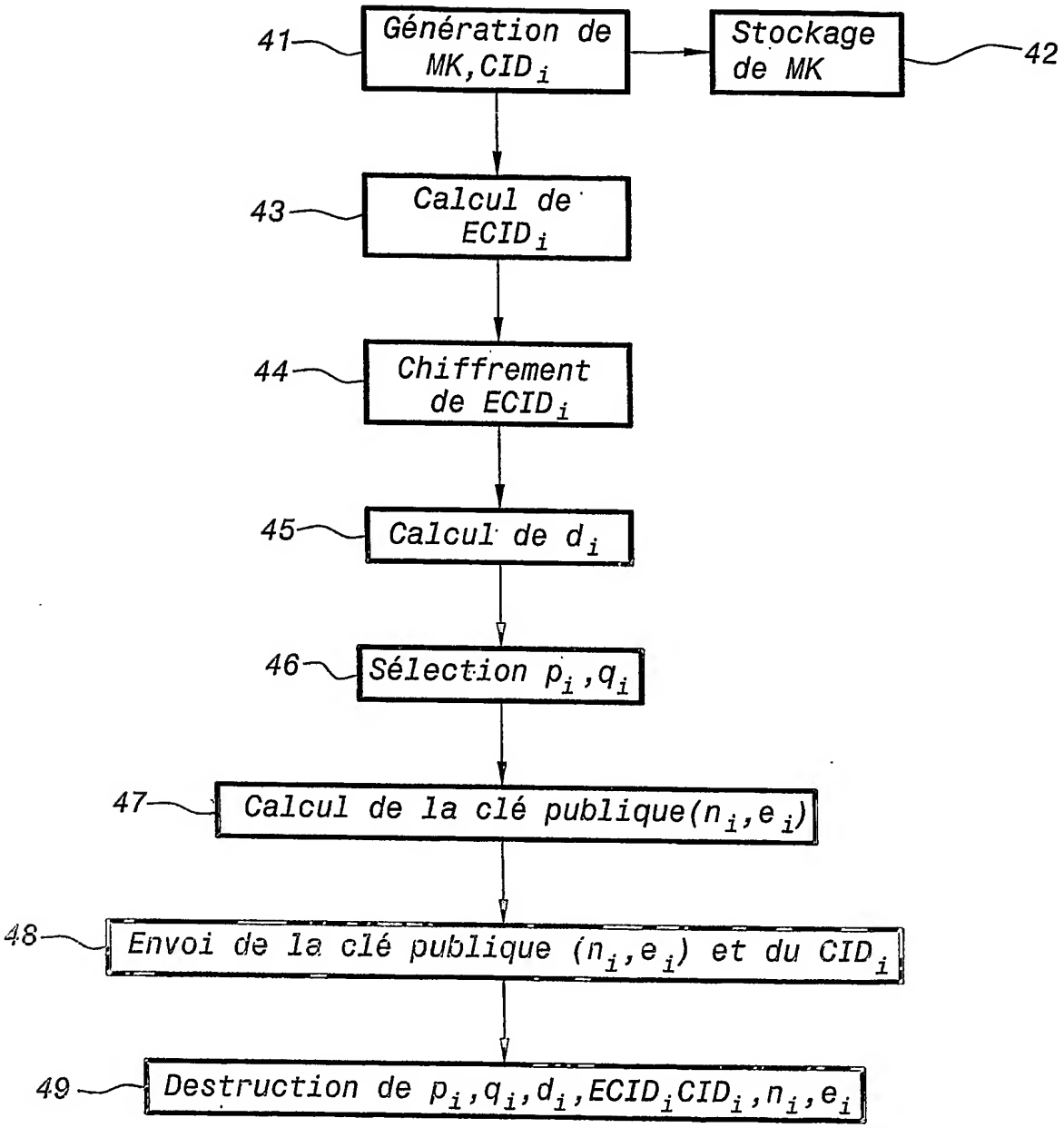
41
Génération de MK, CID_i
Stockage de MK
42
43
Calcul de $ECID_i$
44
Chiffrement de $ECID_i$
45
Calcul de d_i
46
Sélection p_i, q_i
47
Calcul de la clé publique(n_i, e_i)
48
Envoi de la clé publique (n_i, e_i) et du CID_i
49
Destruction de $p_i, q_i, d_i, ECID_i CID_i, n_i, e_i$

FIG.4

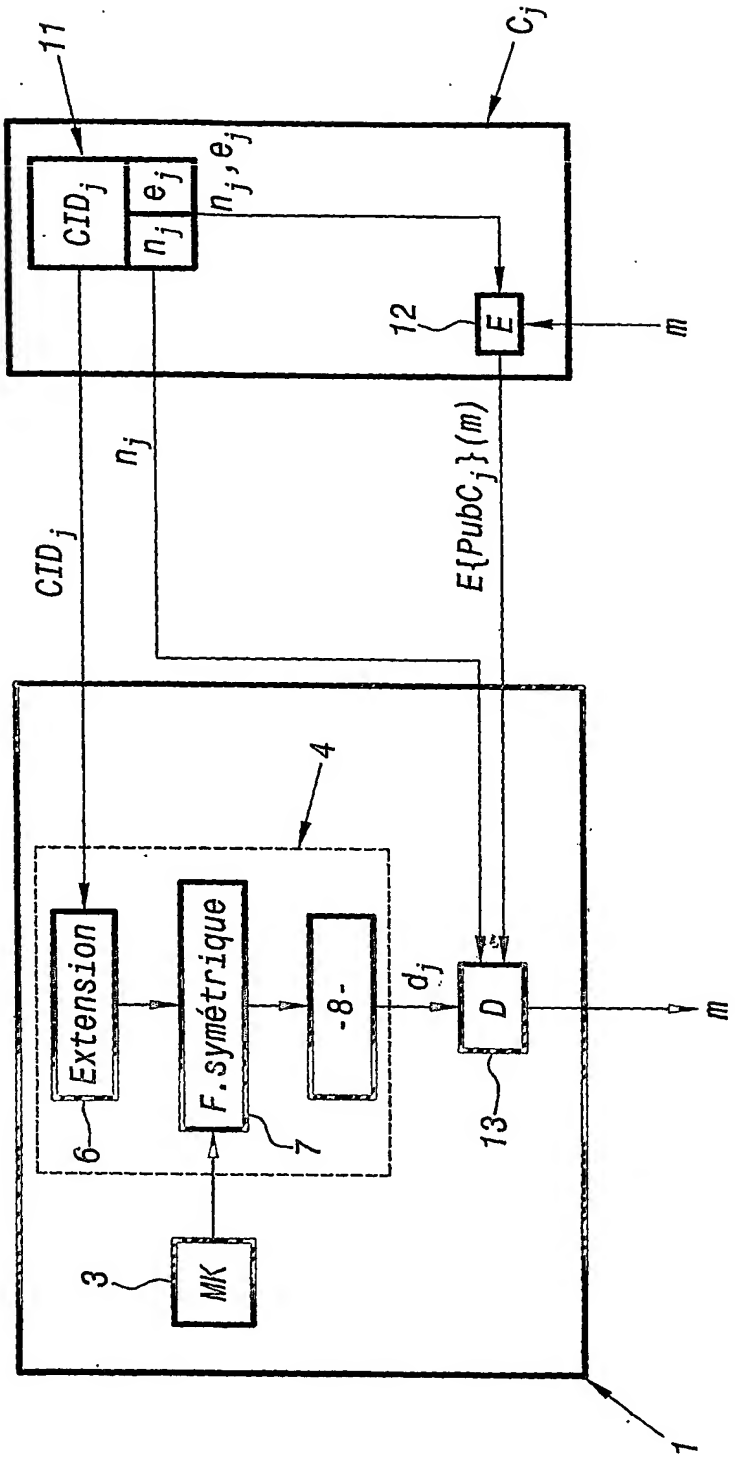
11
C_j
CID_j
e_j
n_j
n_j, e_j
12
E
m
n_j
CID_j
$E\{PubC_j\}(m)$
4
Extension
F.symétrique
-8-
d_j
D
m
6
7
13
3
MK
1

FIG.5

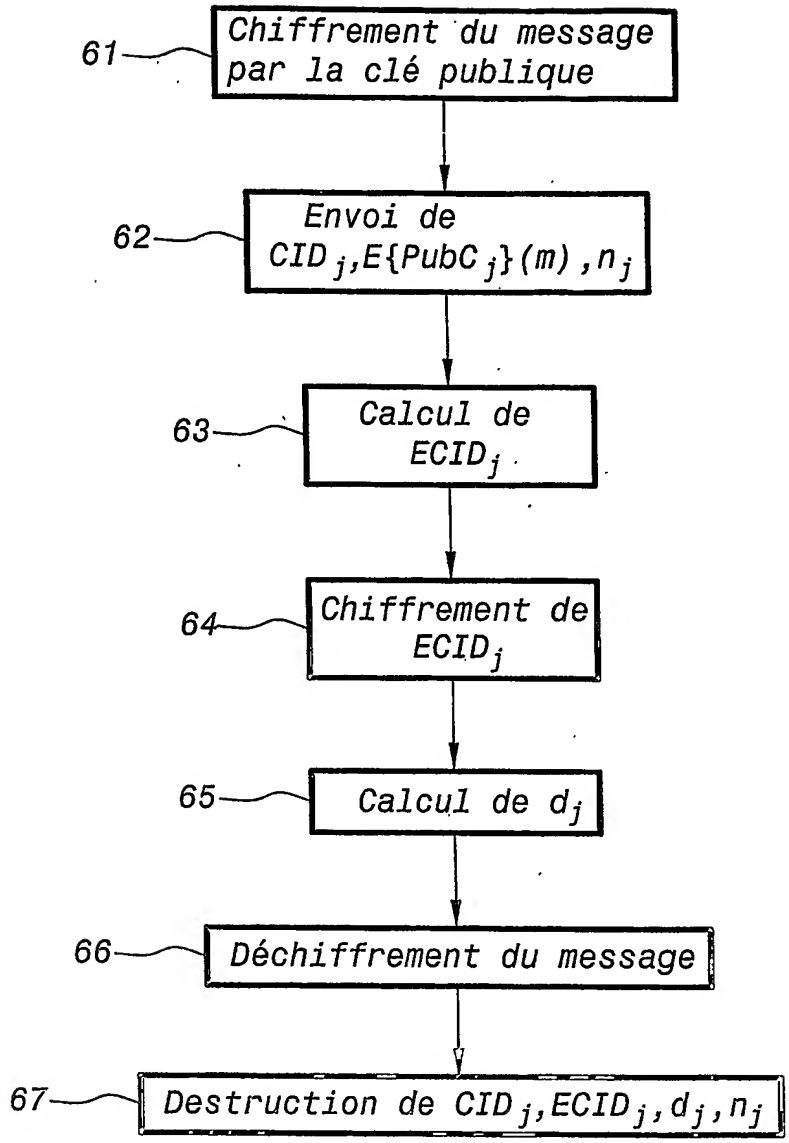
61
Chiffrement du message par la clé publique
62
Envoi de $CID_j, E\{PubC_j\}(m), n_j$
63
Calcul de $ECID_j$
64
Chiffrement de $ECID_j$
65
Calcul de d_j
66
Déchiffrement du message
67
Destruction de $CID_j, ECID_j, d_j, n_j$

FIG.6

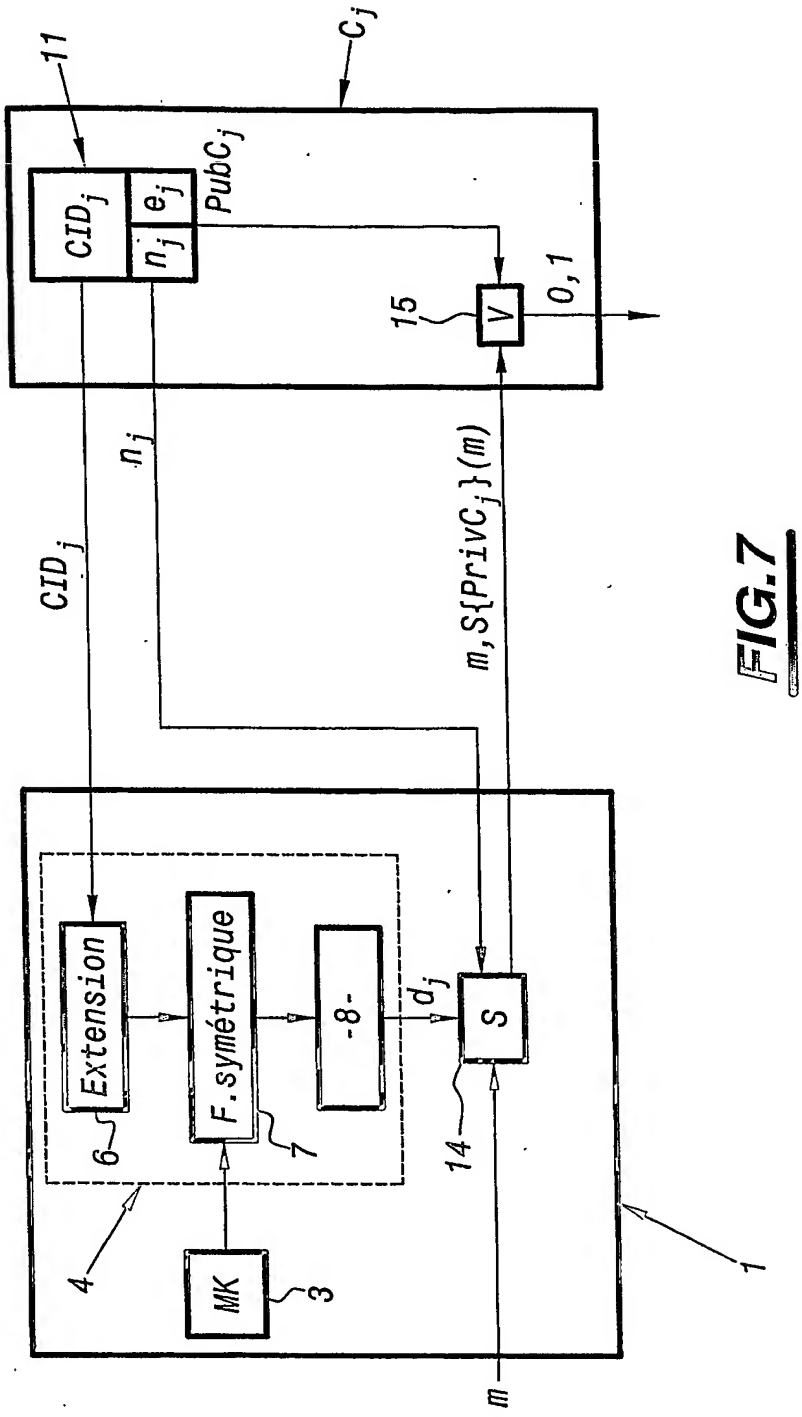
11
C_j
CID_j
e_j
n_j
$PubC_j$
15
V
0,1
n_j
CID_j
$m, S\{PrivC_j\}(m)$
Extension
F.symétrique
-8-
d_j
S
6
7
14
4
MK
3
1
m

FIG.7

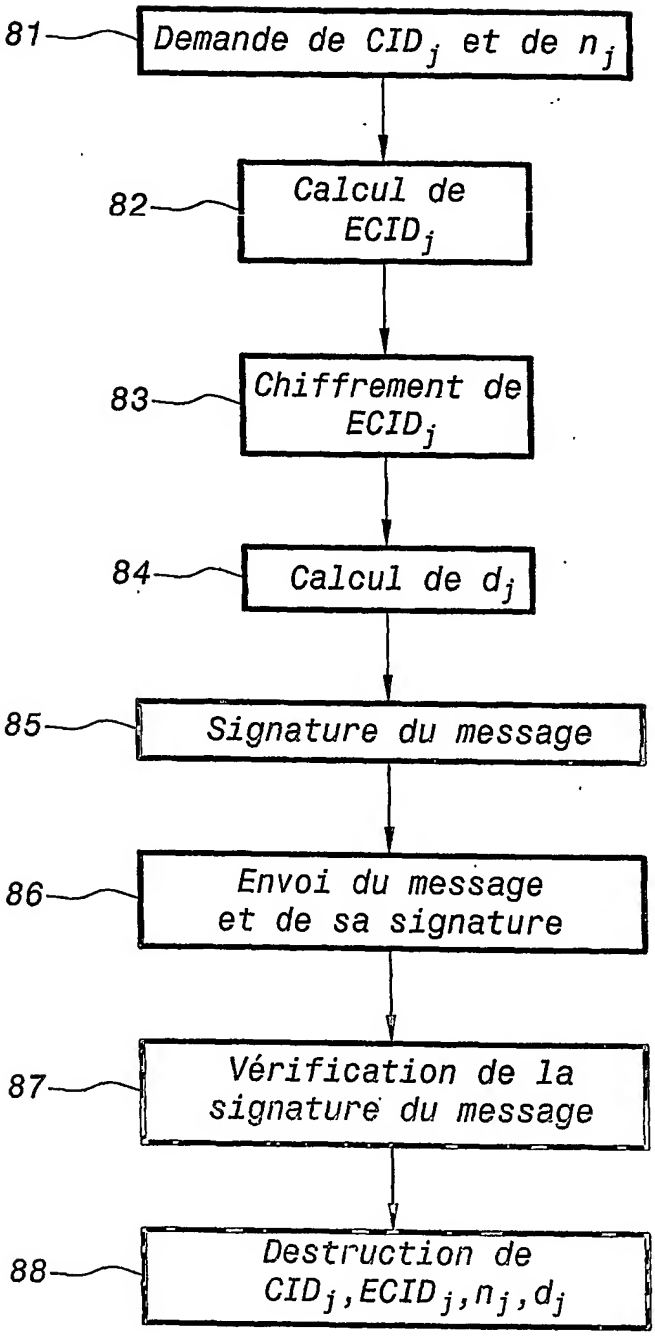
81
Demande de CID_j et de n_j
82
Calcul de $ECID_j$
83
Chiffrement de $ECID_j$
84
Calcul de d_j
85
Signature du message
86
Envoi du message et de sa signature
87
Vérification de la signature du message
88
Destruction de $CID_j, ECID_j, n_j, d_j$

FIG.8

INTERNATIONAL SEARCH REPORT

International Application No
PCT/FR2004/001743

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L9/30

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data, PAJ, INSPEC, IBM-TDB

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 00/72504 A (SOMEREN NICKO VAN ;HARVEY IAN (GB); NCIPHER CORP LTD (GB)) 30 November 2000 (2000-11-30) page 1, line 1 - line 21 page 4, line 13 - last line page 6, line 2 - line 12 figures 3,5	1-19
A	WO 96/05673 A (TRUSTED INFORMATION SYSTEMS IN) 22 February 1996 (1996-02-22) page 10, line 9 - page 11, line 15 page 20, line 1 - page 26, line 4	1-19
A	WO 02/19613 A (HAZARD MICHEL ;CP8 TECHNOLOGIES (FR)) 7 March 2002 (2002-03-07) cited in the application the whole document	1-19

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
3 November 2004	15/11/2004

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Liebhardt, I

Form PCT/ISA/210 (second sheet) (January 2004)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/FR2004/001743

Patent document cited in search report	Publication date	Patent family member(s)		Publication date
WO 0072504 A	30-11-2000	AU	5230500 A	12-12-2000
		CA	2371599 A1	30-11-2000
		EP	1180277 A1	20-02-2002
		WO	0072504 A1	30-11-2000
		JP	2003500922 T	07-01-2003
WO 9605673 A	22-02-1996	US	5557346 A	17-09-1996
		US	5557765 A	17-09-1996
		AU	3321795 A	07-03-1996
		BR	9508548 A	03-11-1998
		CA	2197206 A1	22-02-1996
		CN	1158195 A	27-08-1997
		EP	0775401 A1	28-05-1997
		JP	10508438 T	18-08-1998
		US	5991406 A	23-11-1999
		WO	9605673 A1	22-02-1996
		US	5640454 A	17-06-1997
		US	5745573 A	28-04-1998
		US	5956403 A	21-09-1999
		US	6272632 B1	07-08-2001
WO 0219613 A	07-03-2002	FR	2813467 A1	01-03-2002
		AU	8779701 A	13-03-2002
		WO	0219613 A1	07-03-2002
		TW	535380 B	01-06-2003

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale No
PCT/FR2004/001743

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 7 H04L9/30

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
CIB 7 H04L

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)
EPO-Internal, WPI Data, PAJ, INSPEC, IBM-TDB

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	WO 00/72504 A (SOMEREN NICKO VAN ;HARVEY IAN (GB); NCIPHER CORP LTD (GB)) 30 novembre 2000 (2000-11-30) page 1, ligne 1 - ligne 21 page 4, ligne 13 - dernière ligne page 6, ligne 2 - ligne 12 figures 3,5	1-19
A	WO 96/05673 A (TRUSTED INFORMATION SYSTEMS IN) 22 février 1996 (1996-02-22) page 10, ligne 9 - page 11, ligne 15 page 20, ligne 1 - page 26, ligne 4	1-19
A	WO 02/19613 A (HAZARD MICHEL ;CP8 TECHNOLOGIES (FR)) 7 mars 2002 (2002-03-07) cité dans la demande le document en entier	1-19

☐ Voir la suite du cadre C pour la fin de la liste des documents

☒ Les documents de familles de brevets sont indiqués en annexe

° Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent
"E" document antérieur, mais publié à la date de dépôt international ou après cette date
"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)
"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens
"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée
"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention
"X" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément
"Y" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier
"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
3 novembre 2004	15/11/2004

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Liebhardt, I

Formulaire PCT/ISA/210 (deuxième feuille) (Janvier 2004)

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demande internationale No
PCT/FR2004/001743

Document brevet cité au rapport de recherche		Date de publication	Membre(s) de la famille de brevet(s)		Date de publication
WO 0072504	A	30-11-2000	AU	5230500 A	12-12-2000
			CA	2371599 A1	30-11-2000
			EP	1180277 A1	20-02-2002
			WO	0072504 A1	30-11-2000
			JP	2003500922 T	07-01-2003
WO 9605673	A	22-02-1996	US	5557346 A	17-09-1996
			US	5557765 A	17-09-1996
			AU	3321795 A	07-03-1996
			BR	9508548 A	03-11-1998
			CA	2197206 A1	22-02-1996
			CN	1158195 A	27-08-1997
			EP	0775401 A1	28-05-1997
			JP	10508438 T	18-08-1998
			US	5991406 A	23-11-1999
			WO	9605673 A1	22-02-1996
			US	5640454 A	17-06-1997
			US	5745573 A	28-04-1998
			US	5956403 A	21-09-1999
			US	6272632 B1	07-08-2001
WO 0219613	A	07-03-2002	FR	2813467 A1	01-03-2002
			AU	8779701 A	13-03-2002
			WO	0219613 A1	07-03-2002
			TW	535380 B	01-06-2003